VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Absolvování individuální odborné praxe

Individual Professional Practice in the Company

2016 **Ondřej Klein**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Ondřej Klein**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Tieto Czech s.r.o.
2. Struktura závěrečné zprávy:
a. Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta
b. Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti
c. Zvolený postup řešení zadaných úkolů
d. Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe
e. Znalosti či dovednosti scházející studentovi v průběhu odborné praxe
f. Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vedl odbornou praxi studenta

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Zdeňka Chmelíková, Ph.D.**

Konzultant bakalářské práce: Bc. Radim Hlávka

Datum zadání: 01.09.2015
Datum odevzdání: 29.04.2016

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *8. dubna 2016*

.....
podpis studenta

Poděkování

Rád bych poděkoval vedoucí Ing. Zdence Chmelíkové, Ph.D. za odbornou pomoc a konzultaci při vytváření této bakalářské práce. Dále bych chtěl poděkovat společnosti Tieto Czech s.r.o. za to, že jsem mohl absolvovat praxi právě v této společnosti. A také bych chtěl poděkovat mému konzultantovi a zároveň manažerovi Bc. Radimu Hlávkovi.

Prohlášení zástupce spolupracující právnické nebo fyzické osoby

„Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských programech VŠB-TU Ostrava."

Dne: *8. dubna 2016*

Tieto Czech s.r.o.
28. října 3346/91
702 00 Ostrava - Moravská Ostrava
IČO 64648051 DIČ CZ64648051

.....
podpis zástupce

Abstrakt

V této bakalářské práci popisují absolvování studentské stáže ve společnosti Tieto Czech, která se zabývá vývojem, správou a konzultacemi v IT sektoru. Popisuji oddělení správy sítí této společnosti, jaké technologie a nástroje jsou v ní nejčastěji využívány, a to nejen pro správu sítí, ale taky k mapování síťové infrastruktury a dokumentace.

V bakalářské práci také popisují, na jakých úkolech jsem také po dobu praxe pracoval, jaké byly dosažené výsledky a přínosy zpracovaných úkolů a jaké postupy jsem zvolil při jejích řešení.

Klíčová slova

Tieto, sítě, data centra, praxe, firewall, směrovače, přepínače

Abstract

In this bachelor thesis, I am describing an internship I have attended in the company of Tieto Czech, which is concerned with IT development, administration and consultation. I am focusing on the network administration department of the company - which technologies and tools are used by the employees not only to administrate networks, but also to map network infrastructure and documentation. In the thesis, I am describing the tasks I was working on during the internship, the methods I was using, the results of the tasks and their benefits.

Key words

Tieto, network, data center, intership, router, firewall, switch

Seznam použitých zkratek

Zkratka	Význam
ACL	Access List
ARP	Address Resolution Protocol
CI	Configuration Item
CMDB	Configuration Management Data Base
IP	Internet Protocol
NAT	Network Address Translation
TONE	Tieto Operational Knowledge Engine
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

Seznam ilustrací a seznam tabulek

Obsah

Úvod

Jako bakalářkou práci jsem si vybral provedení odborné praxe v mnou vybrané firmě, kterou se stala firma Tieto Czech. Výběr bakalářského tématu pro mě bylo jasnou volbou, jelikož získané znalosti, poznatky a praxe ve firmě byly pro mne neocenitelným přínosem, hlavně proto, že se jedná o mezinárodní firmu, která se zabývá právě i správou počítačových sítí.

Při výběru pozice v této firmě mne převážně zajímala pozice technického specialisty na síťovém oddělení. Tato oblast je mi velice blízká a vždy mě lákalo a zajímalo, jak vypadá pracovní náplň technika, který spravuje rozsáhlou počítačovou síť. Zaměřil jsem se hlavně na to, jaké nástroje se při správě sítí vyžívají, jaká zařízení jsou při výstavbě síťové infrastruktury využita a jak vypadají síťové technologie a topologie a jak jsou využity mezi daty centra a koncovými body sítí.

Hlavním přínosem této bakalářské práce jsem viděl ve zdokonalení mých znalosti a nabytí mnoha praktických zkušeností, které bych mohl v budoucnu využít ve svůj prospěch při uplatnění na trhu práce a posléze v budoucím povolání.

1 O společnosti

Společnost Tieto je největším dodavatel IT služeb pro soukromý a veřejný sektor ve Skandinávii. Svými službami pokrývá mnoho segmentům, od průmyslového až po segment finanční či vládní. Jedná se o finskou firmu, založenou koncem 60. let se sídlem v Helsinkách s ročními tržbami 1,5 miliard eur, zaměstnává 13 000 expertů a působí ve více než 20-ti zemích světa.

Tieto Czech je jednou z poboček společnosti Tieto, která zaměstnává přibližně 2000 expertů v oblasti IT a je třetí největší pobočkou této firmy, když první dvě místa zaujímá Finsko a Švédsko. S těmito parametry se může pyšnit jako jeden z největších zaměstnavatelů v oblasti IT služeb a největším v Moravskoslezském kraji. [3]

1.1 Historie firmy

1.1.1 Společnost Tietotehdas Oy

Společnost Tietotehdas Oy vznikla ve finském Espoo v roce 1968. V začátcích zajišťovala vývoj a údržbu IT systémů především pro finskou Union Bank a její zákazníky a také pro lesní průmysl. Portfolio zákazníků v 70. letech rostlo a firma postupně rozšířila své zaměření ze sálových počítačů a softwaru i na osobní počítače a vývoj IT systémů.

V 90. letech zaznamenala rychlý rozvoj díky akvizicím, fúzím a vstupu do strategických aliancí. V roce 1995 změnila své jméno na TT Tieto a v roce 1998 na Tieto. V roce 1996 výrazně pronikla do sektoru telekomunikací akvizicí společnosti Avancer. Od roku 1999, kdy se spojily společnosti Tieto a Enator, nesla jméno TietoEnator.

V průběhu minulého desetiletí se naplno projevila globalizace IT průmyslu a společnost rozšířila své mezinárodní působení. V roce 2004 otevřela první off-shore pobočku v České republice. S příchodem indických hráčů na severoevropský trh zesílila konkurence. Od roku 2007 se firma znovu zaměřuje na severoevropský trh. Zároveň si ale ponechala svůj globální vliv ve vybraných odvětvích, především v telekomunikacích. S podporou horizontálních operací a nárůstem počtu zaměstnanců v off-shore zemích změnila v roce 2009 svou průmyslově orientovanou strukturu na matrixovou strukturu vedení v jednotlivých zemích, průmyslových odvětvích a globálních službách. Do roku 2010 výrazně posílila působení v off-shore zemích.

1.1.2 Společnost Enator

Skupina Enator vznikla v roce 1995 fúzí s firmou Celsius a.s., kterou koupila v letech 1991 až 1994. Do roku 1994 se o IT operace staraly tři dceřiné společnosti - Telub, Enator a Dialog. Fúze dceřiných společností vedla k výrazné restrukturalizaci, dokončené v roce 1997. Na jaře 1996 byla společnost zapsána na stockholmské burze pod názvem Enator, v roce 1998 Enator posílil díky akvizicím společnost získala 51 % akcií ve stockholmské konzultační firmě Programmera. Dále převzala dvě malé IT firmy - norský Kvatro Telecom a německý SoftProjekt - a prodala své operace v Enator Telemekanik. V dubnu 1999 společnost Enator koupil dánský NetDesign.

Finská korporace Tieto a švédská společnost Enator se spojily 7. července 1999. Od 26. března 2009 nese společnost název Tieto Corporation.

Společnost Tieto Czech vstoupila na český trh v roce 2001 a v roce 2004 otevřela své softwarové centrum v Ostravě. V roce 2011 se podařilo společnosti vybudovat stabilní zázemí přibližně pro dva a půl tisíce zaměstnanců v centru Ostravy, kde byla vystavěná budova Tieto Towers.[4]

1.2 Oblast působení na trhu

Společnost Tieto působí v oblasti informačních komunikací, vývoji a konzultací dostupných řešení. Tieto svým zákazníkům poskytuje vývoj softwaru podle jejich požadavků a stálou podporu tohoto softwaru. Dále poskytuje konzultace možných řešení, vhodných pro zákazníka. V neposlední řadě Tieto poskytuje svým zákazníkům podporu již nasazených řešení v síťové oblasti a její správu. Mezi zákazníky Tieta patří velké skandinávské společnosti, působící v oblasti financí, zdravotnictví, dřevozpracujícího průmyslu a taktéž města a vlády.

Hlavním úkolem oddělení, na kterém jsem byl zařazen, byla správa sítí, které byly určeny pro zákazníka a interní sítě společnosti Tieto, včetně sítí, navržených pro fungování v data centrech. Síťové oddělení se dále dělí na tým, který poskytuje neustálou podporu pro důležité zákazníky. Druhý tým síťového oddělení se zabývá podporou zákazníků, kteří jsou pod neustálou správou společnosti. Za tyto zákazníky je daný techniky zodpovědný a poskytuje jim podporu v oblasti řešení problémů, které mají dopad na zákaznickou síť. A také spravuje síť, kdy zajišťuje nasazení nových zařízení do sítě nebo změny, které mají být na síti provedeny.

1.3 Struktura společnosti

Hlavní zastoupení společnosti Tieto je ve Finsku, kde je také hlavní pobočka a vedení. Společnost pak má několik desítek poboček. Výkonným ředitelem společnosti Tieto je Kimmo Alkio. Výkonným viceprezidentem společnosti Tieto je Ari Karppinen. Jeden z viceprezidentem společnosti je Kimmo Alkio. Ředitelem oddělení „Infrastructure Foundation Services“ je Christoph Lindemann, pod které jsem spadal hierarchicky i já. Generálním ředitelem české pobočky Tieto je momentálně Petr Lukasík. Hlavním manažerem, zodpovědným za oddělení správu sítí v Česku, je Martin Hlista. Dále je toto oddělení rozděleno na menší týmy a já jsem působil v týmu Radima Hlávky.

2 Pracovní zařazení

Při výběru praxe jsem vyhledával společnosti, které se zaměřují na počítačové sítě, jejich správu a budování. Vybral jsem si společnost Tieto Czech s.r.o., která se zabývá správou a konzultacemi v IT sektoru. O volné pozici jsem se dozvěděl od spolužáka, které již v této společnosti pracoval. Absolvoval jsem dva pohovory s personalistkou, která pro mě domluvila další kolo pohovoru s manažery, kde jsem musel prokázat své znalosti a orientaci v počítačové síti.

Po přijetí jsem byl přiřazen na pozici technického specialisty v oblasti počítačových sítí. Připojil jsem se k týmu Radima Hlávky, který byl pro mne manažerem i tutorem a který mě seznámil s týmem a vysvětili mi, za co budu zodpovědný a zařídil základní trénink, abych se orientoval v síťové struktuře společnosti Tieto. Po dobu celé praxe jsem se zapojoval do projektů, které mi byly zadány manažery, kteří byli zodpovědní za jednotlivé části síťové struktury. Na zadaných úkolech jsem spolupracoval se svými kolegy, kteří byli taktéž na stáží ve společnosti Tieto.

3 Zadané úkoly:

- Správa CMDB - Náplní toho úkolu byla správa databáze TONE, ve které jsou vedena všechna zařízení, které společnost Tieto spravuje.
- Kontrola kapacity klíčových přepínačů v data centrech - V tomto úkolu bylo zapotřebí vytvořit přehled využité kapacity jednotlivých přepínačů, které se nacházejí v data centech společnosti Tieto.
- Vytvoření podkladů pro výměnu síťového jádra - V rámci tohoto úkolu bylo potřeba vytvoření podkladů pro plánovanou výměnu bez komplikací.
- Vypracování přehledu o využité kapacitě WAN směrovače Juniper MX80-T - Bylo potřeba vypracovat jasný přehled o tom, jak jsou využité WAN směrovače v data centrech společnosti Tieta.
- Rezervace IP adres pro nasazení nových zálohovacích serverů - Rezervace IP adres v nástroji, kterým společnosti Tieto disponuje pro jednotlivé virtuální sítě a konfigurace firewallu FortiGate.

4 Zvolený postup při řešení zadaných úkolů

4.1 Vypracování přehledu o využité kapacitě WAN směrovače Juniper MX80-T

4.1.1 Základní popis úkolu

Jedním ze zadaných úkoly bylo vypracování jasného a srozumitelného přehledu využití kapacit WAN směrovačů. V tomto případě se jednalo o hraniční směrovače od společnosti Juniper, které využívá společnost Tieto pro jednu ze svých síťových struktur, kterých je v této společnosti hned několik. Pro tvorbu těchto struktur se využívají zařízení společnosti Cisco a Juniper. Zařízení Juniper jsou separované v logické struktuře sítě. Mým úkolem bylo vypracovat přehled využití těchto směrovačů.

4.1.2 Směrovač

Směrovače jsou aktivní síťové prvky, které pracují na síťové vrstvě ISO/OSI modelu. Směrovače se taky označují jako router. Směrovače rozděluji sítě a zajištují směrování packetu mezi těmi sítěmi. Směrování probíhá na základě IP adres, které jsou přiřazené na rozhraní směrovače a na připojeném zařízení, které pracuje na síťové vrstvě.

Ke směrování packetů se využívají směrovací protokoly. Směrování můžeme mít statické - v tomto případě je za konfiguraci směrování a výběr cesty od zdroje k cíli zodpovědný správce sítě. Dále známe směrování dynamické za využití směrovacích protokolů, které se děli na "link-state vector" a "distace vector". Dynamické směrovací protokoly volí nejlepší cesty na základě jejich typu. "Link-state vector" protokoly vyvolí nejvhodnější cestu od zdroje k cíli na základě paramentu linek, které jsou dostupné. Mezi tyto parametry patří jejich propustnost a celkově zatížení. Mezi protokoly "link state vector" patří protokoly OSPF, IGRP. Druhou skupinou směrovacích protokolů jsou protokoly "distace vector"- ty volí nejkratší cestu v sítí, podle počtu přeskoků. Přičemž přeskokem myslíme přeposlání packetu mezi směrovači. Při každém přeskoku se sníží počet možných přeskoků, a to je na začátku 15 možných přeskoků. Po překročení tohoto omezení je cesta neplatná.

Směrovače v sítí mohou také fungovat jako firewall při využití filtrace packetu neboli ACL. Avšak ve větších sítích, jako ve společnosti Tieto, se takto směrovače nevyužívají. [1]

Společnost Tieto využívá směrovače společnosti Cisco a Juniper.

4.1.3 Popis směrovače

Směrovač Juniper MX80-T se skládá ze čtyř 10 gigabitových vestavěných modulů pro připojení důležitých linek, dvaceti gigabitových slotů pro připojení SPF modulů a dvou vestavěných SFP modulů. Při vypracování přehledu jsem se řídil za pomoci schématu pro směrovač Juniper MX80-T Obrázek 1.1.

Zařízení od společnosti Juniper využívají svého vlastního operačního systému. Tento operační systém se nazývá JUNOS. Operační systém je stavěn na unixovém základu FreeBSD. Výhodou toho operačního systému je rozdělení paměti pro každý aktivní proces. Tím se systém stává odolnějším a méně náchylnějším proti selhání celého systému. [8]

Obrázek 1.1: *Přední strana směrovače Juniper MX80-T*

4.1.4 Způsob zpracování

Za pomoci výpisu konfiguračních souboru z daných směrovačů jsem vytvořil přehlednou tabulku, která obsahovala název daného směrovače a několik informativních tabulek, které obsahovaly výpis všech dostupných modulů a rozhraní na směrovači. Pro každé z těchto rozhraní jsem získal ze směrovače připojené moduly a aktivní linky, které měly aktivní připojení nebo byly zapnuty administrátorem.

Výpis všech rozhraní bylo dosaženo za pomoci příkazu:

```
show chassis hardware
```

Také bylo nutné zjistit popis rozhraní, aby bylo zřejmé, k čemu je dané rozhraní připojeno. Popis rozhraní na směrovači lze zjistit za pomoci příkazu:

```
show interfaces description
```

Tabulky pro každý směrovač obsahovaly výpis všech SFP modulů a dostupných slotů. Ke každému slotu jsem zjistil typ připojeného SFP modulu, stav administrace a linky a popis pro dané rozhraní.

4.1.5 Výsledek vypracovaného úkolu

Mnou vypracované podklady byli použity pro přehlednost situace využití daných směrovačů. Z přehledu se dalo jasně vyčíst, kolik je dostupných slotů popřípadě modulů a kolik je jich využito a za jakým účelem. V některých případech byly moduly rezervovány pro další použití.

Tento přehled posloužil při pomoci budoucí optimalizace nově připojených linek. Také teoreticky mohl sloužit k optimalizaci nákladů a přehlednější správu těchto směrovačů. Technici tak dostali jasný přehled o stavu jednotlivých směrovačů a zda je rozhraní právě využíváno.

4.2 Kontrola kapacity klíčových přepínačů v data centrech

4.2.1 Popis zadaného úkolu

Jeden ze zadaných úkolu byla pomoc při optimalizaci klíčových přepínačů. Zadaná práce spočívala ve vypracování tabulky pro každý přepínač v daném data centru a daném jádře síťové struktury. V každém sítovém jádru se nacházelo několik přepínačů, buď od společnosti Cisco nebo Juniper, v závislosti na typu síťového jádra a jeho využití.

Síťové jádro je logická struktura, oddělující jednotlivé sítě, a to podle jejího účelu nebo použité technologie. Takto jsou síťová jádra oddělená ve společnosti Tieto. Podle typu služeb, pro které je toto jádro navrženo, jsou řešený záložní přepínače a kvalita poskytujících linek. Právě nad těmi jádry, která jsou rozmístěna v několika data centrech, se kontrolovala využitá kapacita jednotlivých přepínačů.

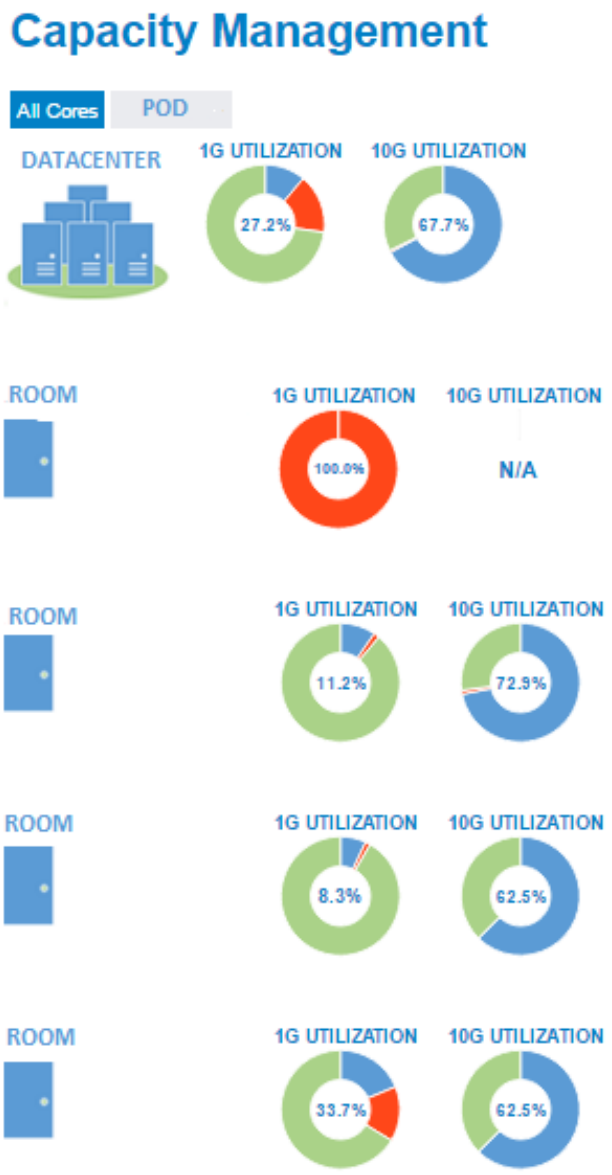
4.2.2 **Popis přepínače**

Přepínače jsou aktivní prvky v sítí, které pracují na linkové vrstvě. Tato zařízení disponují větším počtem rozhraní, například Ethernet, a tak jsou vhodné pro připojení vícero hostů v síti, nejčastěji v rozmezí od 4 do 48 portů. Přepínače se řídí podle zdrojové a cílové MAC adresy, což je fyzickou adresou každého rozhraní, která je unikátní a neměná. Přepínač rozesílá data na základě cílové MAC adresy, obsažené v rámci, který přijal. Přepínače jsou rychlé, a právě proto jsou vhodné pro použití v data centrech. Použitím přepínačů se snižuje kolizní doména.

Na přepínači můžeme také nastavit zabezpečení, a to v podobě VLAN (Virtuální LAN sítí). Jedná se druh zabezpečení na linkové vrstvě, kdy jsou porty přepínače přiřazené do určené oblasti VLAN. V této oblasti se nachází pouze rámce, který patří do příslušné virtuální sítě. Tímto se dá rozdělit provoz a také vytvořit jistý druh zabezpečení v sítí, které využívají převážně přepínačů.

4.2.3 **Tieto Network Manager**

Nástroj Tieto Network Manager je vyvinut automatizačním týmem společnosti Tieto, který je součástí síťového oddělení. Tento nástroj je nástavbou pro nástroj společnosti HP, HP Network Automation, který poskytuje společnost Hewlett-Packard pro síťovou správu a právě tento nástroj Tieto Network Manager rozšiřuje a poskytuje všem technikům, spravujícím síťovou strukturu, jasný přehled o stavu jednotlivých zařízení a výpis rozhraní a stavu tohoto rozhraní. Tento nástroj má usnadnit veškerou správu síťových zařízení. Nástroj obsahuje mnoho funkcí jako například správu VLAN, správu přirazených IP adresa anebo seznam zařízení a jejich komponentů, jako jsou zdroje, ventilátory a podobné komponenty. K zařízení také patří clustery neboli virtuální šasi a tato „zařízení“ se skládají z několika fyzických zařízení, která fungují jako záloha. Tyto clustery obsahuji nejčastěji dvě nebo tři fyzická zařízení, která fungují jako horká záloha v případě výpadku primárního zařízení. Z nástroje je také možnost zjistit jednotlivé modulární prvky zařízení, včetně všech důležitých informací, jako jsou data instalace nebo sériová čísla. V neposlední řadě obsahuje nástroj Tieto Network Manager správu kapacity pro jednotlivá data centra společnosti Tieto, které jsou vyobrazeny v interaktivním provedení.



Obrázek 1.2: *Rozhraní nástroje Tieto Network Manager*

4.2.4 Postup pří vypracování úkolu

Společnost Tieto disponuje hned několika data centry, které se nacházejí převážně ve skandinávských zemích. V každém z data center se vyskytuje hned několik klíčových přepínačů, pro které bylo nutné vytvořit tabulku. Tabulky byly vytvořeny pomoci výpisu z nástroje Tieto Network Manager, kdy tento nástroj mi poskytoval důležité nástroje o všech rozhraních a jejich stavu, zda je daný port aktivní a zda je připojená aktivní linka. Dále obsahoval popis všech dostupných portů, tento údaj byl pro mou práci velice důležitý. Na základě popisu jsem rozhodoval, zda je dané rozhraní dostupné a je možné ho označit pro budoucí použití. Pro popis portů byl již zavedený řád, podle kterého by se popis rozhraní měl řídit. Avšak ne vždy daný technik tento popis změnil. Proto bylo zapotřebí provést tento úkol. Právě podle zavedených praktik se rozhodoval nástroj Tieto Network Manager, zda je port dostupný nebo ne. Ale jelikož se mohlo se stát, že informace, které jsou v popisu, již nejsou aktuální,

bylo zapotřebí všechny porty, které neměly aktivní linku nebo byly vypnuty, zkontrolovat. Podle zavedených praktik by měl popis rozhraní obsahovat jméno serveru nebo zařízení, které by mělo být připojeno na tomto síťovém rozhraní. Pokud byl port právě nevyužíván, měl obsahovat v popisu rozhraní slovo "free" neboli, že je volný a je možné ho použít. Nástroj Tieto Network Manager poté rozhodnul, zda je tento portu dostupný nebo nikoliv, a to na základě popisu rozhraní. A proto bylo velice důležité, aby byl popis aktuální a pravdivý a popřípadě, aby byl správně zapsán. Z vypracovaných tabulek jsem dostal přehled všech portů, které byly hlášený jako vypnuty nebo neměly aktivní linku anebo neobsahovaly adekvátní popis rozhraní pro aktuální stav. Pro opravu popisu rozhraní jsem musel z vytvořených tabulek získat jméno zařízení, které mělo být připojeno do daného portu a to pomocí databáze TONE. V této databázi jsem dohledal jméno, které jsem získal z tabulky a na základě incidentu nebo požadavků, které se vázalo k danému zařízení, jsem rozhodl, zda je možno rozhraní na daném přepínači označit jako volné nebo rezervované. Dále mi byla poskytnutá tabulka, které obsahovala všechny přepínače a jejích rozhraní a číslo incidentu nebo požadavků, které se na dané rozhraní vztahovalo. Tato tabulku byla vytvořena techniky, kteří na těch zařízeních pracují nebo pracovali. Avšak nemusela obsahovat vždy aktuální údaje, a proto jsem musel porovnat datum incidentu, zapsaného v této tabulce s posledním incidentem nebo požadavkem, který byl zapsán v databázi TONE. Po vyhodnocení a porovnání těch incidentů nebo požadavků jsem do mnou vypracované tabulky zapsal aktuální informaci o daném stavu.

4.2.5 Výsledek zpracované úlohy

Tabulky, doplněné o aktualizovaný stav, jsem předal kapacity manažerovi, který tyto informace předal dál, pro další ověření některých případů, u kterých nebylo jasné, zda je možné port označit jako rezervovaný nebo dostupný pro další použití. Tyto tabulky byly následně šířeny celým síťovým oddělením společnosti jako dočasné řešení pro aktuální stav jednotlivého využití přepínačů v data centrech. Vypracování těchto tabulek bylo součástí většího projektu, který se zabýval optimalizací použitelnosti portů v data centrech.

4.3 Rezervace IP adres pro nasazení nových zálohovacích serverů

4.3.1 Popis zadaného úkolu

Jedním z úkolů, který mi byl zadán, bylo rezervování IP adres pomoci nástroje IPAM a následná konfigurace sítě pro implementování nových záložních serverů. Nástroj IPAM je ve společnosti Tieto využívám převážně pro rezervování IP adres.

4.3.2 IPAM

V oddělení pro správu sítě se pro rezervování IP adres pro různé VLAN využívá specializovaný nástroj IPAM, který je určen pro tento účel. Jednalo se o databázi, která obsahovala seznam zákazníků. Ke každému zákazníkovi byly přiřazeny určité VLAN. V rámci tohoto úkolu jsem musel dohledat potřebnou VLAN podle identifikačního čísla. Seznam těchto čísel mi byl poskytnut přes nástroj TONE za pomoci ticketu. Podle čísla VLAN jsem dohledal potřebnou VLAN v nástroji IPAM. Tato VLAN obsahovala seznam všech IP jednotlivých podsítí, které byly pro dané VLAN přiřazeny. V tomto seznamu jsem rezervoval potřebných osm IP adres, se kterými se poté pracovalo při implementaci. Nástroj IPAM bude později součásti nového stroje ServisNow, který v brzké době nahraní stávající systém TONE. Toto sloučení později vyšší integritu dat.

4.3.3 Konfigurace přepínačů Cisco Nexus a firewallů FortiGate

Pro správné fungování záložních serverů, pro které jsem v rámci tohoto úkolu rezervoval IP adresy, je nutné zajistit, aby tyto servery komunikovaly společně se servery, které jsou aktivní, takzvaně v produkci. Záložní servery v tomto případě poskytovaly pouze zálohu dat, které jsou na produkčních serverech a nesloužily jako horká záloha. Jelikož tyto servery musí v interní sítí komunikovat, musí se zajistit správná konfigurace zařízení, která se mezi servery nacházejí.

4.3.4 Konfigurace přepínačů

Pro správné fungování bylo nutné nakonfigurovat všechny přepínače, které se nacházejí mezi produkčními servery a zálohovacími servery. Jelikož se jedná o síťovou strukturu, založenou na linkové vrstvě ISO/OSI modelu, je potřeba přiřadit patřičné porty do předpřipravených VLAN. A na směrovačích, kde se tyto VLAN střetávají, přiřadit danou VLAN na trunk linku. Pro zjednodušení této konfigurace společnost Tieto vytvořila nástroj Tieto Network Manager, který spravuje síťová zařízení a je schopen přiřadit na všech přepínačích potřebnou VLAN a přidání potřebné VLAN na trunk linku. Díky tomu nástroji tento krok proběhne najednou a není potřeba konfigurovat každý přepínač zvlášť.

4.3.5 Firewally

Síťový prvek firewallu se v počítačových sítí využívá především pro filtraci paketů, které těmito zařízeními procházejí. Firewall je jeden ze základních bezpečnostních prvků v síti. Firewally se dělí na kontroly komunikace beze stavové a stavové. Beze stavové filtrace rozhodují o průchodu jednotlivých paketů na základě adresy zdroje a cíle, kterou má packet definovanou. Beze stavové firewally pracují na třetí vrstvě modelu ISO/OSI. V menších sítích můžeme využít směrovače, na které můžeme aktivovat službu pro filtraci packetů, a to za využití ACL, které můžeme na směrovači definovat. Stavový firewall pracuje na čtvrté vrstvě a filtruje packety na základě IP adres a portu služeb, které chceme filtrovat.

Firewally mohou zabránit různým typům útoků a průniku do sítě. V sítích se využívají právě proto, aby servery byly ochráněny před případným útokem. A jsou nastaveny tak, aby filtrovaly tyto případné útoky, ale také aby mohli uživatelé z internetu bez problému využívat služeb, které server poskytuje. [1]

4.3.6 Popis firewallu FortiGate 1500D

Další prvek, který bylo potřeba nakonfigurovat, je firewall, který je součástí síťové struktury. Firewall může nahrazovat směrovač, ale hlavně filtruje provoz v síti. V sítí, ve které se nachází zmíněné servery, byly jako firewally použito zařízení od společnosti FortiNet model FortiGate 1500D, jenž je navržen pro použití v data centrech. Tento firewall je typu NGFW (Next-Generation Firewall), prostupnost tohoto firewallu se pohybuje okolo 80 Gb/s. Poskytuje ochranu proti průnikům, tak pokročilými hrozbami. A poskytuje i filtraci provozu na základě obsahu. FortiGate 1500D disponuje 8 porty o rychlosti 10Gb/s a 32 porty o rychlosti 1Gb/s. Celé zařízení pak využívá operačního systému FortiOS 5. Cena tohoto zařízení se pohybuje okolo 25 000 dolarů. [9]

Pro konfiguraci těchto firewallů se dá využít nástroj, který umožňuje správu vícero firewallu stejné společnosti nebo webové rozhraní, které je dostupné na každém firewallu anebo se dá využít příkazové řádky a konfigurovat firewall pomocí příkazů. Pro tento případ jsem využil nástroj pro konfiguraci vícero firewallů přes nástroj FortiGate Manager, který je dostupný po zadání konkrétní adresy v prohlížeči. Poté, co se přihlásíme do nástroje FortiGate Manager, je potřeba uzamknout

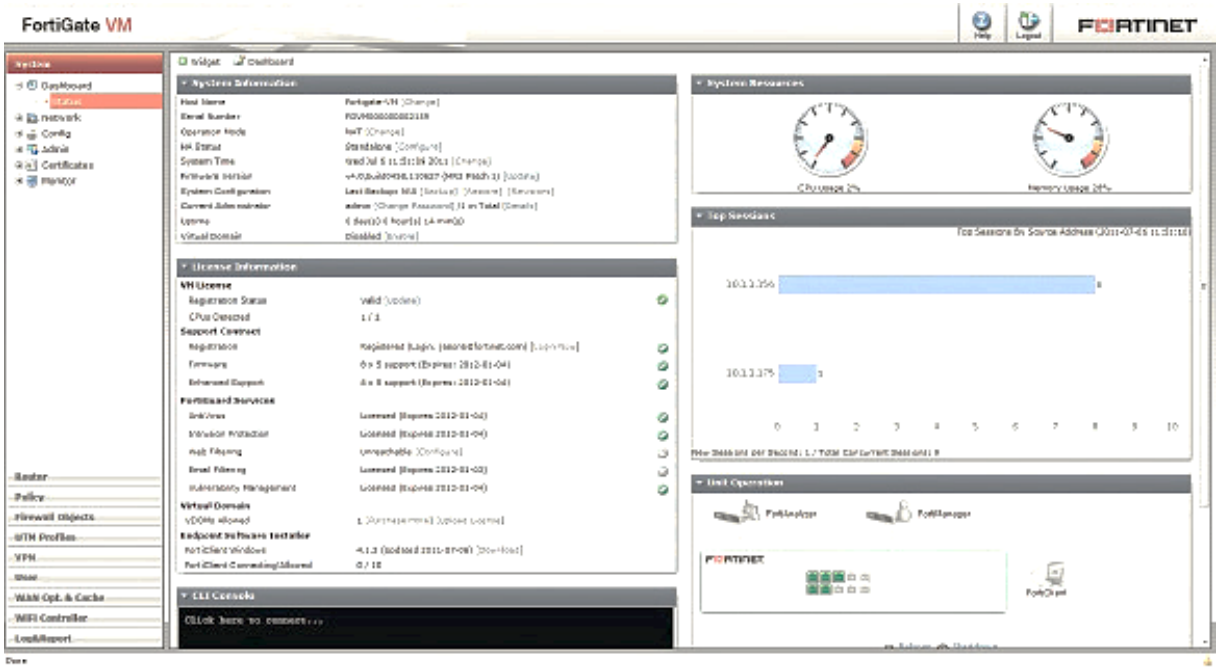
konfigurace na svůj účet. Což zabrání, aby na jednom firewallu probíhalo několik úprav najednou, což sebou nese bezpečnostní riziko přepsání konfigurace. Pokud se takto firewall uzamkne na určitý uživatelský účet, může se firewall konfigurovat právě pouze z tohoto účtu. Uzamknutí je pouze dočasné po dobu, kdy se na firewallu provádí úpravy.

Obrázek 1.3: *Firewall FortiGate 1500D*

4.3.7 **Konfigurace firewallu FortiGate 1500D**

Na firewallu společnosti FortiNet je nutno konfigurovat pravidla, objekty a NAT pro korektní fungování. Na každém fyzickém firewallu jsou definovaný firewally virtuální, pro které se konfigurují specifická pravidla a překládání síťových adres. Na těchto firewallech jsou definovany zóny, do kterých se musí přiřadit rozhraní, na kterém je zařízení připojeno. A proto je potřebné, abychom rozhraní přiřadili do potřebné zóny. Potom je potřeba vytvořit virtuální objekt a virtuální IP adresu. Tento krok je potřebný proto, že v síti se nenacházejí žádné směrovače a proto zde firewall tuto roli zastupuje a má na svém virtuálním rozhraní jednu z adres, kterou jsem rezervoval v nástroji IPAM. Podobné virtuální rozhraní lze implementovat i na směrovačích společnosti Cisco, které lze využívat také pro směrování mezi VLAN. Tato rozhraní na firewallech odpovídají na ARP dotaz, a proto se pro koncový server tváří jako výchozí brána a proto můžeme v této síti využívat firewallů jako výchozích bran. Poté je důležité nastavit překlad síťových adres tak, aby se specifická IP adresa, přeložena na IP adresu s určitou adresou. Pro překlad síťových adres je tady důležité nastavit, jaké rozhraní je interní a externí. Jelikož se jedná o servery a je důležité, aby měly svojí vlastní IP adresu, nastavíme statický překlad síťových adres. Jelikož v tomto případě jsme implementovali tři záložní servery, pro každý se vytvořil statický překlad síťových adres. Těchto několik serverů je potřeba přiřadit do skupiny, pro kterou se budou uplatňovat pravidla pro filtraci síťového provozu. Tento krok se provádí pro přehlednost všech přidaných serverů, jelikož by bylo potřeba při každé změně provádět aktualizaci zvlášť pro každý server, takto stačí uplatnit změnu pouze na tuto skupinu. Pokud jsou vytvořeny všechny předchozí položky a všechny potřebné servery jsou přiřazeny do skupiny, můžeme na tuto skupinu uplatnit pravidla filtrace v síti. Tato pravidla se v ničem neliší od ACL, které jsou uplatňovány na směrovačích, například společnosti Cisco. Tato pravidla obsahují adresu zdroje, popřípadě adresu cíle, dále obsahuje akci, která se provede v případě, že se takový paket dostane na rozhraní firewallů, v tomto případě může jít o akci zahodit nebo přeposlat. Nedílnou součásti tohoto pravidla je také port, který daná služba využívá ke komunikaci a také typ protokolu, který služba využívá. Tato pravidla jsou seskupena a používána pro jednotlivé objekty nebo skupiny, které jsou na firewallu vytvořeny. Aplikovat pravidla můžeme, jak na jednotlivé objekty

i skupiny, avšak využívání skupin je pohodlnější a přehlednější pro správu těch pravidel. V našem případě stačilo přidat skupinu serveru do skupiny pravidel, která se na přiřazené skupiny aplikují. Pravidla pro tento případ již byla vytvořena, jelikož se jednalo o záložní servery, kterých je v této síťové struktuře již několik. A známe všechny požadavky pro správné fungování sítě a filtrování. [5]



Obrázek 1.4: *FortiGate Managment Firewallu*

4.3.8 Aplikovaní změn na Firewallech FortiGate 1500D

Pokud byly všechny změny úspěšné a jsou ověřeny, je potřeba námi provedené změny uplatit na daný firewall. Instalace ověří integritu zadaných dat, pokud je tento krok úspěšný, provede se samotné uplatnění pravidel pro objekty a rozhraní. Po provedení všech potřebných kroků a úspěšné instalaci se může pokračovat v konfiguraci nebo odemknout firewall pro další konfiguraci a poznačit, jaké změny byly provedeny a za jakým účelem. [5]

4.3.9 Výsledek dokončené úlohy

Tento úkol byl součásti změny, která byla prováděna pro dva zákazníky, které společnosti Tieto spravuje, jednalo se o zákazníky EnterCard a Symatec, kteří přišli s požadavkem pro implementování záložních serverů.

4.4 Správa CMDB

4.4.1 Popis zadaného úkolu

Jedním z největších úkolů, který jsem za dobu svého působení zpracovával na praxi, byla správa databáze CMDB, která je součásti nástroje TONE. Hlavní náplní bylo doplnění nebo oprava informací, které jsou v této databázi zaneseny. Tyto informace chyběly z důvodu chyby při vytváření těchto zařízení v databázi. A bylo nutno tyto informace doplnit. Úkol se skládal z několika části.

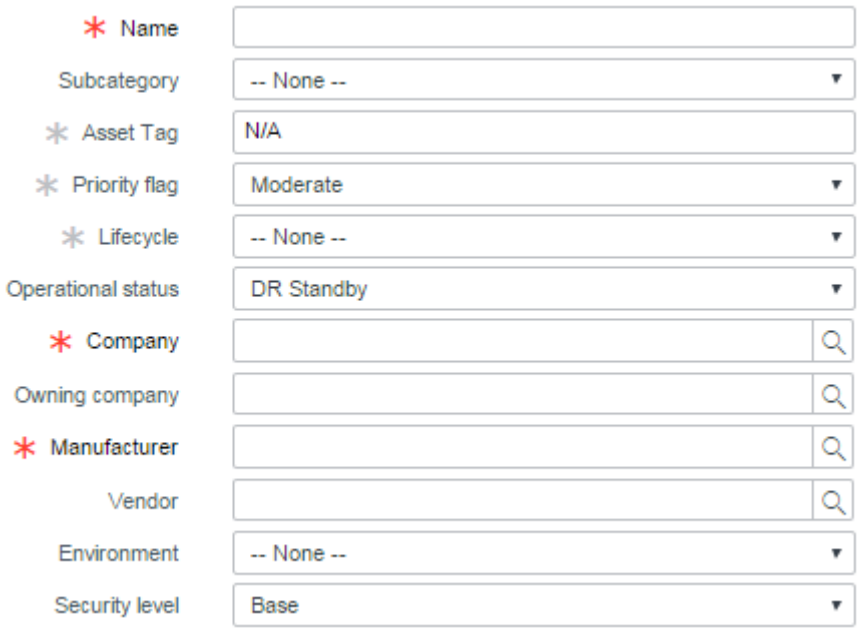
- První částí úkolu bylo doplnění podkategorie jednotlivých zařízení.
- Druhou a největší části toho úkolu bylo doplnění a popřípadě vytvoření lokací v databázi CMDB. Bylo nutné, abych doplnil potřebné informace pro to, aby mohlo být zařízení fyzicky dohledatelné v případě jeho správy, která vyžadovala fyzický zásah. Informace jsem získával od mých kolegů, kteří tato zařízení spravují a jsou za ně zodpovědní.
- Poslední částí bylo ověření integrity dat mezi databází CMDB a daty, poskytované nástrojem TNM, který jsem již výše popisoval. Tento úkol byl nutný, jelikož databáze CMDB je spravována ručně, a proto informace nemusely být aktuální nebo mohly chybět úplně. A proto jsem za pomoci reportu, který byl vygenerován nástrojem pro porovnání databází CMDB s daty nástroje TNM.

4.4.2 **TONE a CMDB**

TONE je základní nástroj, který je ve společnosti Tieto využíván napříč všemi odděleními. Tento nástroj vychází z komerčního nástroje ServiceNow a je přizpůsobený pro požadavky společnosti Tieto. Jedná se o tiketovací systém, který využívají velké společnosti. Používá se pro standardizaci úkolů. Tyto tikety sebou nesou důležité informace o daném úkolu a aktuálním stavu. A následně se předávají mezi patřičnými odděleními ve společnosti. Tiket může být vygenerován některým z monitorovacích systémů

Nástroj CMDB se využívá jako databáze všech zařízení, incidentů, problému, změn a úkolů a je součástí TONE. Všechny tyto záznamy v této databázi jsou mezi sebou propojeny a poskytují všem zaměstnanců celkový přehled. V rámci toho úkolu jsem nejčastěji pracoval s databází CMDB, která je součásti nástroje TONE. V databázi CMDB jsou zaznamenány všechna zařízení, která společnost Tieto spravuje. Tato databáze se dá ještě rozdělit podle tytu zařízení, o které se jedná. Mezi tyto položky se řadí zařízení, jako jsou servery, směrovače, přepínače, data centra a všechna ostatní fyzická zařízení.

Tato zařízení/položky se v databázi CMDB značí jako CI. K těmto CI se vztahují položky, jako jsou incidenty, problémy, změna a platby od zákazníků společnosti Tieta. Nástroj TONE poskytuje pro tato CI přehled závislostí. Při pohledu na jednotlivé CI se můžeme dovědět, jaká zařízení jsou připojená k danému zařízení. Dále taky poskytuje informace o tom, kde se toto zařízení fyzický nachází. Mezi tyto informace patří data centrum místnost v tomto data centru a případně rozvaděč, ve kterém se dané zařízení nachází.



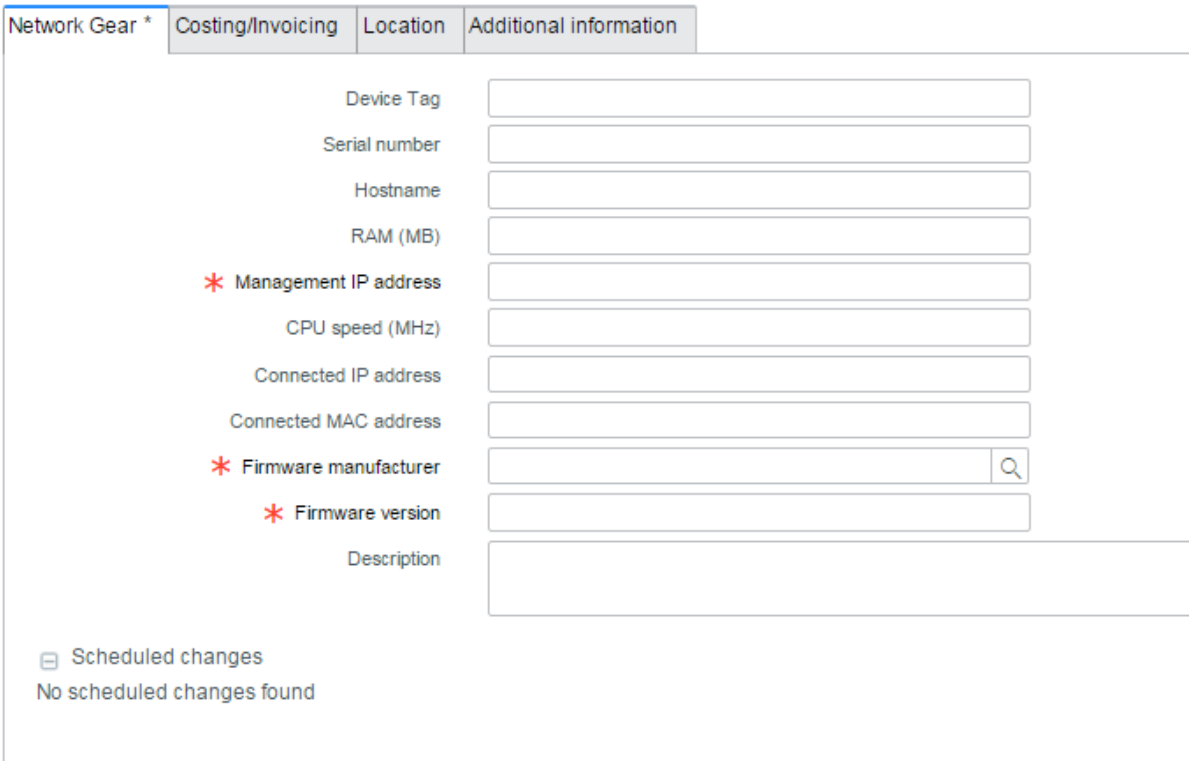
Obrázek 1.5: *Základní informace potřebné při vytváření CI v nástroji TONE*

Na obrázku Obrázek 1.4 je zachycena část stránky, která je součástí formuláře, který se zobrazí pro každé zařízení, které je v databázi TONE zaneseno.

Důležitou položkou v tomto případě je název CI, který se řídí podle jistých pravidel, která jsou součásti návodu, avšak pro odlišné zákazníky jsou odlišná pravidla pro přiřazování jmen. Toto jméno je v CMDB jedinečné. Vždy musí být zřejmé, o jaké zařízení se jedná. Další položkou je podkategorie, informace v tomto poličku jsem doplňoval v jedné z části tohoto úkolu. Další položkou, která je důležitá, je "Priority flag", kdy se jedná o položku, která určuje důležitost CI v hierarchické struktuře, ve které se nachází. Podle této položky se poté tvoří incidenty, které se vztahují k tomu CI a k jeho důležitosti. Další položkou, které se zde nachází a je nutné, aby byla vyplněná, je "Lifecycle". Jedná se o informace, které určuje v jaké stádiu CI je, zda je aktivní nebo probíhá údržba anebo je již smazáno a tím pádem nefunkční. V databází se udržují i informace o zařízení, která již nejsou funkční. V této položce je také možné určit i jiné stavy, jako například "v údržbě", "čeká na instalaci" nebo "na odchodu". Tyto stavy pomáhají technikům se zorientovat, v jaké fázi se momentálně zařízení nachází a odůvodnit případné potíže. Položka "Operational status" určuje, zda je zařízení aktivní nebo neaktivní, popřípadě je v pohotovosti jako záloha. Další nutnou položkou je "Company". Do této položky se zapisuje, pro jakou společnost je zařízení určeno. Tato položka je důležitá v případě, že dojde k problémům, nebo že je nutné provést změnu. V tomto případě lze zjistit, že právě toto zařízení bude mimo provoz a kontaktovat tak zákazníka, že právě jeho se mohou týkat problémy, které mohou nastat. Potřebné informace i položka "Manufacturer". Tato položka nese informaci o výrobci zařízení. Tato informace je důležitá, pokud je nutno kontaktovat podporu výrobce v případě problémů, které jsou například spojeny se softwarovým problémem. Jednou z položek je také "Security level". V této se jedná o informaci, o jaké zařízení se jedná nebo pro jakého zákazníka zařízení je. Společnost Tieto spravuje i několik zákazníků, kteří vyžadují zvýšené zabezpečení, což vyžaduje zvýšenou bezpečnost při manipulaci na těchto zařízeních. S těmi CI mohou pracovat pouze technici, kteří splňují požadavek mít bezpečnostní prověrku. A pracují na místech, která jsou speciálně zabezpečena.

Dalšími položkami, které musí CI obsahovat, jsou informace o tom, kdo zařízení spravuje. Také jsou zde uvedeny informace o oddělení, která zodpovídá za podporu zařízení. Nedílnou součásti je také skupina, která součástí podpory společnosti Tieta. V neposlední řadě je také uvedeno jméno technika, který za dané zařízení zodpovídá.

V případě specifické skupiny CI, které spadají do kategorie síťového zařízení, jsou požadovaný i specifické informace.



Obrázek 1.6: *Potřebné specifické informace pro síťové zařízení*

Specifickými informacemi pro síťová zařízení jsou položky "Serial Number"- do této položky se zadává výrobní číslo daného zařízení. S touto položkou jsem převážně pracoval v poslední části tohoto úkolu, kde jsem ověřoval integritu dat v databázi CMDB a dat poskytnutých nástrojem Tieto Network Manager. Další položkou seznamu, kterou jsem se zabýval v poslední části úkolu, je "Hostname". Dalšími položkami jsou "RAM", které nesou informace o velikosti paměti zařízení. Důležitou položkou je však "Management IP address"- jedná se o IP adresu, která se využívá ke správě zařízení. Dalšími povinnými položkami jsou "Firmware manufacturer" a "Firmware version"- tyto položky obsahují typ firmwaru a verzi, které je aktuálně dostupná na daném zařízení. Tyto položky informují techniky, jaký firmware je aktuálně nainstalován na zařízení a zda již není zastaralý. Tato položka je také potřebná pro případ plánové výměny.

Na obrázku Obrázek 1.5 je vidět i několik karet, které by měly být vyplněny. Pro tento úkol pro mě byla nejpodstatnější záložka "Location". Tato karta obsahuje pouze několik položek, které bylo nutné v mém případě doplnit. Jednalo se o políčka "Country", "Data Center", "Computer Room" a "Rack". Tyto položky nejsou nezbytné, avšak je důležité, aby byly vyplněny pro připadat potřeby fyzického zásahu. Například kvůli výměně nebo fyzické kontrole.

Všechny tyto informace, poskytnuté v záznamu každého CI, jsou důležité pro správu. Jelikož pro každé CI lze v nástroji TONE vytvořit incident, problém nebo výměnu. A tyto události je potřeba vyřešit v co nejkratším čase. A právě dostatek informací může potřebný čas zkrátit. Tyto události jsou provázaný z CI, kterých se týkají. Toto provázání pomáhá při řešení problémů všem technikům. [6]

4.4.3 Řešení zadaného úkolu

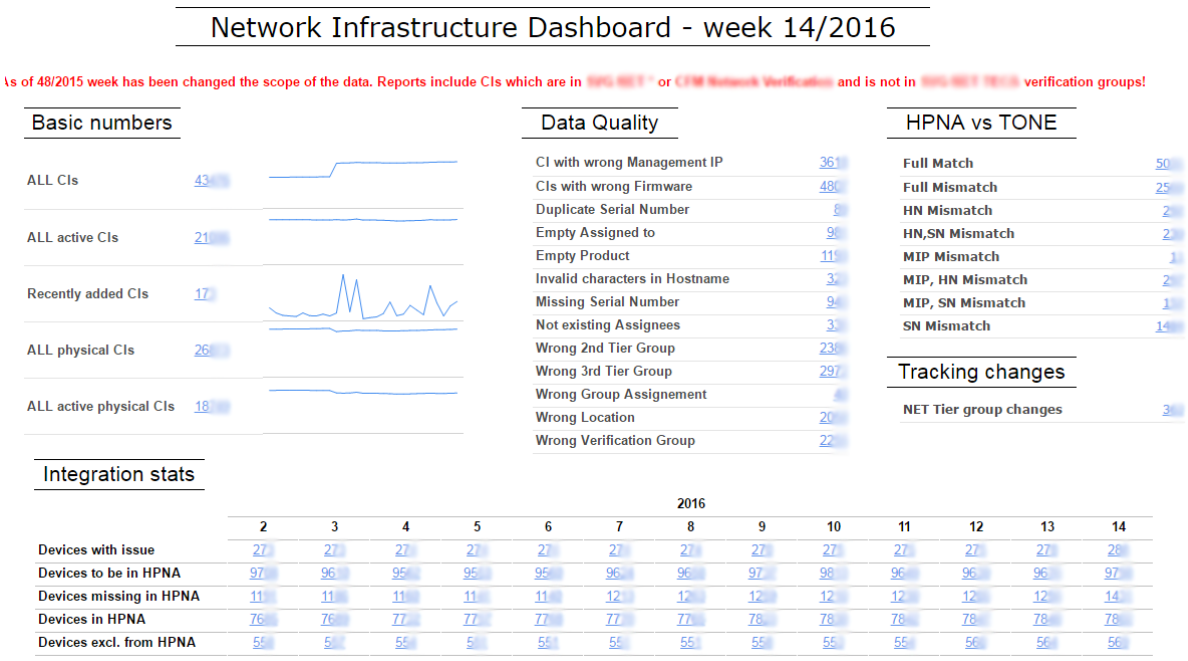
Zadaný úkol byl součásti většího úkolů, který byl zadán pro zkvalitnění informací, poskytnutých nástrojem TONE. Úkol jsem řešil za pomoci reportů, které byly vygenerovány pomoci webové aplikace. Tyto reporty bylo vygenerovány v Excelu a mým úkolem bylo kontrolovat jejich správnost a chybějící informace do databáze CMDB doplnit.

V první části šlo o doplnění podkategorie u CI, u kterých nebyla tato položka vyplněna. Za pomoci vygenerovaného reportu jsem dostal přehledný seznam všech zařízení, u kterých tento problém nastal. V tomto případě se však nejednalo o velký počet zařízení. Položka podkategorie nese informaci, o jaké zařízení se jedná. Zda se jedná o směrovač, přepínač nebo jiné zařízení. Pro doplnění informací jsem musel kontaktovat technika, který byl za dané zařízení zodpovědný. Tento technik mi poskytnul informace, které jsem posléze doplnil. V některých případech jsem tuto informaci nemohl doplnit, jelikož daný typ zařízení nebylo možno vybrat z nabízených možností.

Druhá část úkolu byla velice rozsáhlá. Před začátkem vypracování úkolu seznam obsahoval přibližně 4500 položek, u kterých bylo nutno doplnit informace. V případě druhého úkolu se již jednalo o doplnění lokace, na které se zařízení nachází. Jak jsem již zmínil, tato informace je potřeba pro případ fyzického zásahu na zařízení, jakou jsou např. vizuální kontrola zařízení, výměna zařízení za jiné nebo jeho odstranění. A jelikož mezi zákazníky Tieta patří společnosti, které disponují obrovskými areály, umožní právě přesná adresa při hledání daného zařízení v tomto areálu nebo určité oblasti. A tak pomůže zkrátit čas při řešení případného problému. Při řešení úkolu jsem využíval vygenerované tabulky za pomoci webového nástroje, stejný jaký byl použit v první části úkolu. Tabulka obsahovala informace, jako byly název CI, podkategorie, název zákazníka a jméno technika, který toto zařízení spravuje. Toto jméno však nemuselo vypovídat, že technik ví přesnou polohu. V některý případech dokonce jméno technika chybělo úplně. Proto jsem musel využit seznamu zákazníků a techniků, kteří pro dané zákazníky mají kontinuální podporu. O tyto informace jsem tabulku doplnil a dané techniky jsem kontaktoval přes interní komunikátor. Ostatní technici mi poskytli informace o lokaci. Pokud však bylo zařízení umístěno v data centrech společnosti Tieto, bylo potřeba doplnit konkrétní informace o počítačové místnosti s rozvaděči, kde se zařízení nachází. V případě, že byly potíže se zjištění této lokace, bylo potřeba kontaktovat technika, který byl zodpovědný za správu data centra. A ten mi poskytnul přesnou lokaci zařízení.

Avšak v případě většiny zařízení se jednalo o zařízení, která nebyla v data centrech společnosti Tieto, ale nacházela se v zákaznických data centrech. (V tomto případě se zákaznickými data centry mínilo umístění jednoho nebo několika zařízení.) V tomto případě bylo nutné zjistit konkrétní adresu zařízení a také data centra. Jelikož data centra, která nejsou pod správou Tieta, musí být součástí databáze CMDB. A tyto zákaznické data centra musí být také řádně provázaná se zařízeními, která jsou v těchto data centrech umístěna. V mnoha případech však tato data centra v databázi CMDB chyběla úplně, a proto bylo potřeba vytvořit nové data centrum, což bylo součástí mého úkolu.

Pro vytváření nových lokací jsem musel kontaktovat administrátory databáze TONE. Jako první krok bylo nutné zanést získané informace do předpřipravené tabulky, která byla navržena pro tento způsob jako jeden z nástrojů standardizace dat. Tato tabulka vygenerovala název adresy, která musela být vytvořena v databázi TONE. Vytváření adresy v databázi obstarávají administrátoři této databáze. A proto jsem tuto tabulku poslal na příslušné oddělení a to na základě zaslané tabulky vytvořilo odpovídající adresy. Tyto adresy musely obsahovat stát, město, ulici a také GPS souřadnice. Jakmile byly adresy vytvořeny, bylo potřeba na těchto adresách vytvořit zákaznické data centrum. Data centrum se v nástroji TONE, vytváří stejně, jako jakékoliv CI v databázi. Takto vytvořené CI muselo obsahovat vytvořenou adresu, dále obsahovalo název data centra, který se řídil pravidly, která určovala, jak by název měl vypadat. A to nejčastěji ve tvaru "DC", dále následoval název společnosti, pro kterou je data centrum určeno a jako poslední město, ve kterém se data centrum nacházelo. Výsledný název pak mohl vypadat takto "DC TIETO Ostrava". Mezi další potřebné informace při vytváření CI pro data centrum se řadí zákazník, pro kterého je DC vytvořeno, a také informace o tom, zda je data centrum aktivní a stále v produkci. Dalšími informace jsou informace, které určují pro jaké oddělení společnosti Tieto budou určovaný zprávy spojené s tímto data centrem a jaké týmy budou pověřeny za správu tohoto data centra. Po vyplnění všech těchto položek bylo data centrum vytvořeno a zařazeno do databáze CMDB. Jako poslední krok bylo nutno přiřadit toto nově vytvořené data centrum k zařízením neboli CI, u kterého tato informace chyběla.



Obrázek 1.7: *Webové rozhraní nástroje pro generování reportů*

Poslední částí zadaného úkolu bylo zkontrolovat správnost údajů mezi databází CMDB a údajem, poskytnutým nástrojem TNM. Údaje poskytnuté nástrojem TNM jsou získaný přímo ze zařízení, a proto se dají považovat za aktuálnější a správnější, jelikož se do nich nepromítá lidský faktor. A proto bylo důležité zkontrolovat, zda se údaje shodují, a pokud tomu tak nebylo, tak proč tomu tak je. Díky reportu, který byl vygenerován za pomoci stejné webové aplikace, kterou jsem využíval již v předchozích částech, jsem porovnával záznamy mezi databází CMDB a nástrojem TNM, byla

poskytnuta všechna zařízení, u kterých se problém s nesprávnými údaji objevil. V případě, kdy k této neshodě došlo, bylo zapotřebí tento údaj opravit. V tomto úkolu se jednalo o neshodu v sériových číslech nebo zařízení. Z vygenerovaného souboru jsem vyhledával všechna zařízení v nástroji TNM. Nástroj mi poskytnul potřebné informace, a to buď potřebné sériové číslo, popřípadě správný hostname. Tento získaný údaj jsem doplnil do databáze CMDB, v některých případech jsem konzultoval změnu s technikem, který byl zodpovědný za správu zařízení, zda je tato změna přípustná. Nejčastěji jsem se setkal se špatným značením zařízení, které pracovalo v režimu clusteru. Takový cluster se většinou skládal z několik zařízení, nejčastěji ze dvou fyzických zařízení, které byla označena pod jedním názvem, a tak se chovala jako jedno fyzické zařízení. V síťové struktuře působilo jako horká záloha pro případ výpadku primárního zařízení. Hostname zařízení se řídilo podle jednoduchých pravidel, a to tak, že cluster se značil názvem zařízení, například ROUTER a fyzické zařízení, které tento cluster obsahoval, byla označena jako ROUTER1 a ROUTER2.

Dále jsem se zabýval nesprávným sériovým číslem, které bylo zaneseno do databáze CMDB. Zařízení, kterých se tento problém týkal, bylo nutné zkontrolovat v nástroji TNM a číslo opravit nebo doplnit v databázi CMDB. Avšak při řešení úkolu jsem se setkal s problémem, který se vyskytnul v nástroji TNM. Jelikož cluster je obsahuje dvě a více zařízení avšak pouze jedno zařízení je aktivní. A právě nástroj vypisuje právě pouze aktivní zařízení nacházející se v clusteru. A proto bylo těžké rozlišit, o které zařízení se aktuálně jedná. Zvlášť v případech, kdy se jednalo o víc než tři zařízení, která byla zaštítěna v jednom clusteru.

4.4.4 Výsledek zpracovaného úkolu

Jak jsem již zmínil, tento zadaný úkol byl součástí většího úkolu, který se týkal zlepšení a zkvalitnění informací, které se nacházely v databázi CMDB. Tento počin by měl pomoci všem zaměstnancům, kteří zařízení spravují při řešení problémů a orientaci jak v síťové struktuře, tak fyzické struktuře umístění zařízení. Zařízení neboli CI, která měla doplněny všechny potřebné informace, by měla být označena jako ověřená a označená stupnicí kvality poskytovaných informací. Pro společnosti jako je Tieto je zásadní aby databáze, které využívá, měli maximální počet aktuálních informací ve svých záznamech.

Výsledek mé práce jde jednoznačně označit počtem CI, které se nacházely na začátku a na konci vykonaní práce ve vygenerovaném reportu. Na začátku zpracování tohoto úkolu měl vygenerovaný seznam s chybějícími lokacemi okolo 4500 položek, u kterých lokace chyběla. V závěrečné fázi se tento seznam zredukoval na přibližně 2000 položek. Z toho většína měla označení, ze kterého bylo jasné, proč toto zařízení je v tomto vygenerovaném seznamu.

Jedním z faktoru, který snížil počet vyřešených položek je, že počet zařízení se každým týdnem zvětšuje, a proto vygenerovaný soubor vždy obsahoval nová zařízení, která se předtím v tomto reportu nenacházela.

4.5 Vytvoření podkladů pro výměnu síťového jádra

4.5.1 Popis zadaného úkolu

Jedním ze zadaných úkolů bylo pomoci při připravované migraci síťového jádra. Tento úkol zahrnoval práci s tabulkami, poskytnutými jedním z techniků, který vedl tuto výměnu. Tabulky obsahovaly výpis podsítí, které se v daném síťovém jádru nacházely. Obsahovaly také NAT objekty,

které se nacházely na firewallech a také výpis všech VRF. Druhá tabulka obsahovala výpis směrovacích tabulek. Bylo nutné, abychom jednotlivé záznamy provázali a dohledali potřebné informace pro jednotlivá pravidla, která se na firewallech nacházela. Tento úkol se skládal ze dvou části - první se zaměřovala na propojování jednotlivých podsítí, směrovacích tabulek a firewallů, - druhá část se zabývala přiřazováním k jednotlivým pravidlům, odpovídající NAT objektům.

4.5.2 Virtuální směrování a přeposílání (VRF)

Virtuální směrování a přeposílání je IP technologie, která dovoluje existenci vícero směrovacích tabulek na jednom fyzickém zařízení. Jelikož jsou jednotlivé směrovací instance na sobě nezávislé, je možné využít překrývajících se podsítí nebo stejných IP adres. Virtuální směrování a přeposílání je možné odkazovat na směrovací instance, které existují v jedné nebo víc instancí pro VPN nebo hraniční směrovač. [2]

4.5.3 Překlad síťových adres (NAT)

NAT neboli překlad síťových adres je nástroj, který se využívá pro překlad nejčastěji neveřejných IP adres na IP adresy veřejné. Jeho použití se považuje za bezpečnostní prvek v síti. Překlad může probíhat v poměru 1:1, a to znamená, že k jedné určitě stanici je přiřazena určitá veřejné IP adresa, též se označuje jako statický překlad adres. V poměru n:m se přiřazuji IP adresy z určitého rozsahu a jsou stanicím přiřazeny dynamicky, z toho také vyplývá název dynamický překlad. Také můžeme využit tzv. přetíženého překladu, kdy je větší počet neveřejných IP adres přeložen pouze na jednu IP adresu za využití portů, které jsou při průchodu jednotlivým spojením přiřazeny při průchodu NAT. Pokud se stanice nacházejí za NAT, nejsou z vnější sítě dosažitelné, pokud není zajištěn právě překlad statický.

4.5.4 Vypracování zadaného úkolu

Pro tyto úkoly byly naprosto důležité podklady, které mi byly poskytnuty. V tabulce, která obsahovala kompletní výpis z virtuálních směrovacích tabulek mi posloužila pro vyhledávání a orientaci v síťové struktuře daného síťového jádra. V druhé tabulce byly uvedeny IP adresy podsítí, které se v síťovém jádře nachází. Tyto podsítě jsem vyhledával v první tabulce. Jelikož některé IP adresy podsítí měly větší prefix, bylo nutné dohledat, zda tato podsíť nespadá do větší podsítě, která má nižší prefix. Například pokud jsem v tabulce s IP adresami narazil na podsíť, která měla prefix 28, musel jsem zkontrolovat, zda tato podsíť není součásti větší podsítě, která měla například prefix 24 nebo 16. Jakmile jsem si byl jistý správnosti nalezeného záznamu ve směrovacích tabulkách, přiradil jsem hostname firewallu k odpovídajícím podsítím, které se nacházely v druhé tabulce. Tímto vznikl přehled firewallů spadají do určité podsítě.

Druhá tabulka také obsahovala seznam všech pravidel pro filtraci provozu, která byla uplatněna pro jednotlivé NAT objekty. Při práci na tomto úkolu jsem se setkal s dalšími typy NAT. Mezi, které patřil například source/destination NAT a také staticky/dynamický NAT. Při analýze jednotlivých NAT pravidel jsem setkal se všemi variantami. Seznam všech NAT objektů, které byly uplatněny ve firewallech, byly součástí druhé tabulky. Seznam těchto pravidel obsahoval informace o zdrojové IP adrese, cílové IP adresa a také typu služby, pro které se mají adresy překládat. Tyto NAT objekty se skládaly z pravidel pro filtraci síťového provozu. Součásti úkolu bylo také k těmto NAT objektům přiřadit odpovídající pravidla pro filtraci. K tomuto přiřazováni jsem využíval webové aplikace od společnosti AlgoSec, která dokázala ověřit, zda je zadané pravidlo pro filtraci provozu součástí

některého z NAT objektů. Pokud tomu tak bylo, aplikace zobrazila všechny NAT objekty, ve kterých se toto pravidlo vyskytuje.

4.5.5 **Výsledek zpracovaného úkolu**

Tento úkol byl součástí většího úkolu, který byl zpracován týmem techniků společností Tieto. Tito technici využili mnou vypracované podklady pro rychlou kontrolu po provedení migrace jednoho ze síťových jader. Podklady také pomohly pro nastavování jednotlivých nových NAT objektů, což ve výsledku mělo pozitivní dopad při provádění těchto úloh.

5 Uplatněné teoretické a praktické znalosti

Po dobu praxe ve společnosti Tieto jsem se setkával převážně s počítačovými sítěmi, ve kterých jsem zužitkoval znalosti převážně z předmětů, které jsou na tuto problematiku zaměřeny. Především předměty jako jsou počítačové sítě nebo telekomunikační sítě. Z těchto předmětů jsem zužitkoval převážně znalosti, které se týkaly zařízení Cisco, které jsem získal v předmětu Počítačové sítě I. S těmi zařízeními jsem se setkával ve společnosti nejčastěji, jelikož větší část jejich struktur je založena na řešení od společnosti Cisco. Užitečné mi také byly znalosti řešení, které poskytuje společnost Cisco pro sítě, které jsou stavěny na jejich zařízeních. Dál jsem zužitkoval teoretické znalosti základních síťových pojmů. Jako například znalost virtuální sítě VLAN, podsítí, směrování a beze stavovou filtraci packetů. Všechny tyto znalosti mi pomohly při řešení jednotlivých jichž zmíněných úkolech.

Znalosti získané v průběhu studia mi také pomohly při jednotlivých školeních, které jsem po dobu působení praxe absolvoval, abych se mohl zapojit do týmu. Ty mi byli užitečné, pokud se jednalo o zaškolování s aplikacemi, se kterými jsem se poté měl setkat na pracovišti. Převážně se jednalo o rozšířené znalosti síťové tématiky.

6 Scházející znalosti

Po dobu praxe byla pro mě větší překážkou absolutní neznalost zařízení od firem, které nejsou stejně rozšířené, jako je společnost Cisco. V mém případě se nejčastěji jednalo o zařízení od společnosti Juniper, který poskytuje obdobná řešení jako společnost Cisco. O jaké prostředí se jedná a jaké základní příkazy se na těchto zařízeních objevuji.

Dalšími nedostatky pro mě byla správa firewallu a jaký vyznám může mít v síťové struktuře firewall. Jelikož jsem se setkal s konfiguracemi těchto zařízení, bylo nutné pochopit a nastudovat, jak se firewall konfiguruje. A jaký význam mají jednotlivé položky, které je nutné zahrnout při konfiguraci.

Znalosti mi taky scházely v souvislosti se strukturami data center. A to, jak takové data centrum je navrženo a jaké mají tyto topologie výhody a nevýhody. Jaké technologie se pro tyto data centra využívají. A zařízení, se kterými se můžu v těchto data centrech setkat, jako jsou například load balancery nebo DWDM technologie.

7 Časová náročnost

Název úlohy	Čas potřebný k vypracování ve dnech
Správa CMDB	30
Rezervace IP adres	7
Kontrola přepínačů v data centrech	10
Přehled hraničních směrovačů	1
Pomoci při migraci	10

Tabulka 1.1: *Časová náročnost*

Závěr

Praxe ve společnosti Tieto byla pro mě přínosem především pro získání praktických zkušeností v oblasti počítačových sítí. Přínosem pro mě také byla práce v nadnárodní společnosti, která se řadí mezi jednu z největší společností v České republice. Po dobu praxe trvající bezmála 8 měsíců jsem se setkal se spoustou různých reálných situací a poznal jsem chod společnosti a především oddělení pro správu sítí. Právě počítačové sítě byl obor, ve které jsem se chtěl zdokonalit a poznat, jak se spravují rozsáhlé sítě, jakými společnosti Tieto disponuje. Tato praxe byla pro mě přínosem a výhodou na trhu práce, jelikož společnost mi poskytla mnoho cenných zkušeností, a to jak teoretických tak praktických. V průběhu zpracování jednotlivých úkolů jsem se setkal s různými zařízeními, která se využívají pro větší sítě, jakou jsou firewally, které se převážně využívají v data centrech.

Přínosem mi také byly tréninky, které mi společnost Tieto poskytla. Ať už se jednalo o tréninky, které byly povinné při nástupu na pozici technického specialisty, tak tréninky, které jsem absolvoval v průběhu absolvování praxe, jako byly například správa firewallu FortiGate anebo různé nástroje pro správu nebo mapování sítě. Poznal jsem mnoho možných způsobů, jaké se dají v praxi využít a budou mi v mé budoucí kariéře přínosem.

Použitá literatura

[1] LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010. ISBN 978-80-251-2359-1.

[2] Virtual Routing and Forwarding. Cisco Active Network Abstraction Reference Guide [online]. 2014 [cit. 2016-03-1]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7/reference/guide/ANARefGuide37/vrf.html

[3] Informace o Tieto. Tieto - IT, výzkum a vývoj a poradenství. [online]. 2015 [cit. 2016-04-01]. Dostupné z: http://www.tieto.cz/tieto-o-nas

[4] Historie společnosti Tieto. Historie - Tieto - Czech Republic [online]. 2015 [cit. 2016-04-01]. Dostupné z: http://www.tieto.cz/tieto-o-nas/historie-tieto-czech-republic

[5] LINDHOLM, Anders. Netbackup implementation guide. Helsinki, 2015.

[6] Tieto Operational Knowledge Engine User's Manual. 2016.

[7] ABHISHEK, Kumar, MATERNA, Miroslav (ed.). CMDB User Giude. 2015.

[8] Juniper – Junos operating system fundamentals. Další IT blog [online]. 2014 [cit. 2016-04-08]. Dostupné z: http://papezt.cz/juniper-user-interface-options/

[9] Nový výkonný podnikový firewall FortiGate-1500D. CIO Business World.cz [online]. 2014 [cit. 2016-04-08]. Dostupné z: http://businessworld.cz/bezpecnost/novy-vykonny-podnikovy-firewall-fortigate-1500d-11697